Fortinet 2013 Cybercrime Report

Cybercriminals Today Mirror Legitimate Business Processes

Long gone are the days when cybercrime was tantamount to teenage miscreants causing mischief in their parents' basement. Today, as any commercial enterprise, cybercrime has evolved into a complex, highly organized hierarchy involving leaders, engineers, infantry, and hired money mules. Looking from the outside in, there's little to distinguish cybercrime organizations from any other business.

Like any legitimate commercial enterprise, each player has a designated role or function to perform. And each job is necessary in order to create the desired good that turns the wheels of the machine. The mission? Like any other business, it's profitability. Or, in some cases, retribution.

The fundamental laws of economics apply here as well. The deliverables run the range from consulting, services, and advertising to a myriad of programs that serve as the "product." The more features and/or more complex the service offered, the higher the price.

However, while they are well-established, these crimeware syndicates are not completely insurmountable. Successful take-downs of high-profile botnets have served to present major setbacks to cybercriminals. Some nations have even participated in collaborative efforts to prevent cybercriminals from registering domains. These are often in the form of working groups, such as the Conficker or Mariposa working group.

Looking ahead, efforts from law enforcement and domain registrars will continue to curb cybercrime efforts. This will likely be coordinated through CERT groups and relations with security firms. However, a more comprehensive, multi-layered approach to security will be key in bolstering that effort.

The Organizational Structure of Crime-as-a-Service

By all appearances, Crime-as-a-Service (CaaS) is a very well-oiled machine, thanks to a wide network of players that fulfill specific functions and propel the mission of the organization forward.

The Executive Suite

The organization's "executives" make decisions, oversee operations, and ensure that everything runs smoothly. Just as with legitimate businesses, these executives set up the original business model and infrastructure. Once they get the operation off the ground, they then move to a business development role and hand off the 'dirty work' to the infantry and are not involved with launching attacks.

However, if the leadership of a criminal syndicate could be likened to a company's C-level bench, then the workers running affiliate programs could be likened to a company's middle managers. Middle managers are typically recruited through "old boy" networks and/or underground forums. The affiliate's responsibility is simply to infect as many machines as he/she can. They can attempt to do this on their own or they can work with recruiters to hire people to do the dirty work for them.

The Recruiters

Also crucial to the organization are recruiters. Many times, people at the affiliate level are the ones who are devising and executing an infection campaign; however, larger organizations will actually actively recruit and manage others (the infantry) to infect the machines for them. Large-scale operations have recruiters that typically set up recruitment programs (these are known as affiliate programs), which are funded by the cyber criminal network executives.

The Infantry

At the bottom of the chain of command are the infantry. These are the ground-level forces that initiate the actual infection on a user's machine. In 2008, John Stewart, director of malware research at SecureWorks disclosed that prolific cybercriminals are most likely netting up to $5 million per year by controlling a large botnet of malware infected PCs. There are a number of ways infantry can infect a person's computer including, but not limited to, email links, Search Engine Optimization attacks, poisoned PDFs, and compromised Websites. Cyber criminals also leverage social networking links, malicious Websites, and poisoned media such as Flash and QuickTime.

Help Wanted

In order to help recruit infantry, recruiters and affiliate program leads will establish fully-realized Web portals. Many of these portals *(See Figure 1)*

Cybercriminal Pay Rates

Consulting services such as botnet setup
($350-$400)

Infection/spreading services
(~$100 per 1K installs)

Botnets & Rentals
[Direct Denial of Service (DDoS) $535 for 5 hours a day for one week], email spam ($40 / 20K emails) and Web spam ($2/30 posts)

Quality Assurance vs. Detection
(Crypters, Scanners - $10 per month)

Affiliate Programs
($5k per day is possible)

Onshore & Offshore Hosting – Virtual Private Servers
($6 per month)

Bulletproof/Fast Flux hosting and VPNs & reverse proxies
($3 per month)

Blackhat Search Engine Optimization (SEO)
($80 for 20K spammed backlinks)

Inter-Carrier Money Exchange & Mule services
(25% commission)

CAPTCHA Breaking
($1/1000 CAPTCHAs)—Done through recruited humans

Crimeware Upgrade Modules:
Using Zeus Modules as an example, range anywhere from $500 to $10

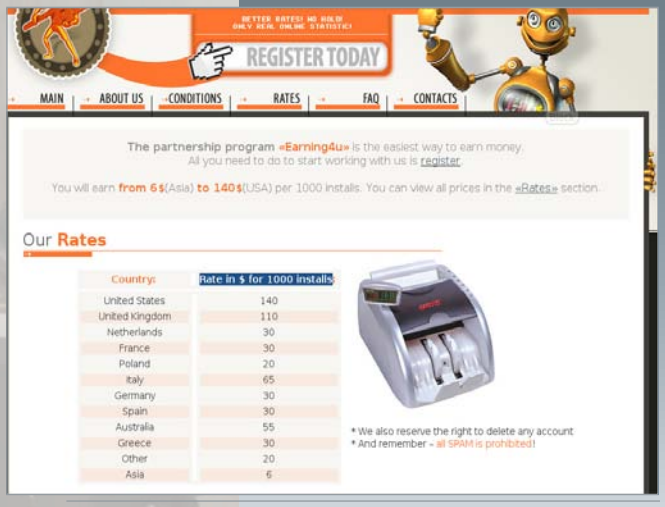


Figure 1: Example of earnings potential for affiliates

originate in Russia ("Partnerkas") and are closed communities made accessible by invite only. The others, depending on where they are in the world and what the laws of that particular country are, are open to the public. Oftentimes to protect themselves, open portals include disclaimers on the site that say, "We do not allow spam or other illicit methods for machine infection." These are typically in place to put the legal responsibility on the infantry. These portals provide the infantry with all of the necessary information they require to begin an infection campaign. Among other things, these tools include illicit software, support forums, payment rates and tracking and a method in which to receive payments upon completing a certain number of infections. *(See Figure 2)*

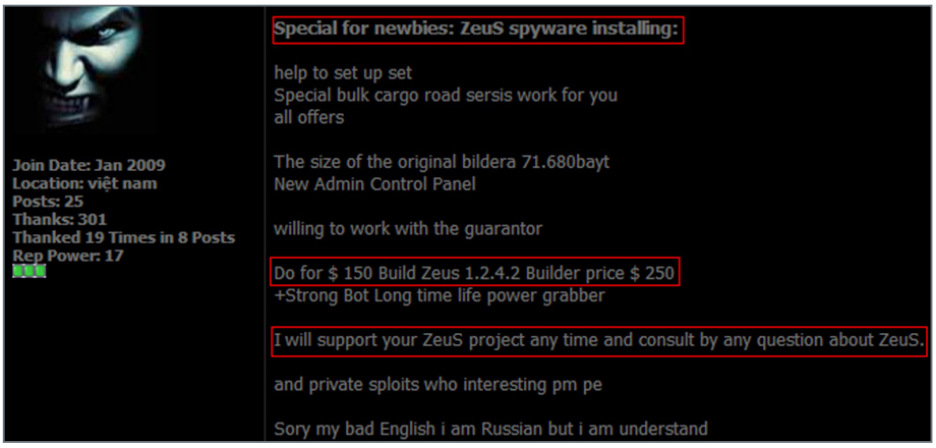


Figure 3: Cybercriminals offer support services for botnet

There are also open portals that only operate with legitimate advertisement programs and affiliates (Advertisement programs, although not malicious, are usually considered a nuisance due to their behavior, such as bundling unwanted adware with software downloads). However, it can be tough to distinguish – seemingly legitimate portals may offer non-advertised, malicious products to distribute.

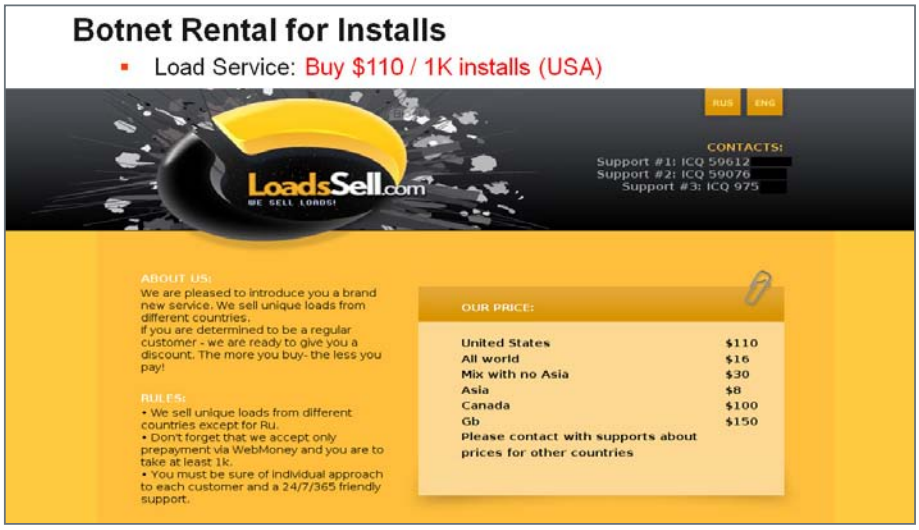


Figure 2: Example of botnet rental pricing configuration

Program Development

To properly arm the infantry, recruiters/affiliates must develop the programs used to infect other systems. These applications include, but are not limited to, fake antivirus software, ransomware, and even botnets.

Once the malicious software is installed on a machine, it can begin to do a number of things, such as downloading additional malware onto a victim's system, stealing credentials and data from banks and social networking sites and even detect and remove competing malware on the infected user's system. Malicious software can also be used to proxy malicious traffic for the crime syndicate, house data on behalf of cybercriminals, encrypt critical data for ransom and generate revenue through click fraud (clicking on advertisements throughout the Web on the users' behalf).

Promotion

As in legitimate businesses, it's not enough to have a good product. The profitability of an organization will also be contingent upon its ability to promote its goods and raise awareness about the services it has to offer. One of the most practical ways to recruit infantry is through a general-purpose advertising campaign. These ads could appear on Internet job boards, hacking message forums, and underground IRC chat channels. They might have a headline that reads, "Want to earn money online?". *(See Figure 3)*

Crime Services

Crime services are offered by middle-men at the infantry or syndicate level as well, as a way to expand their money-making opportunities. There are a wide variety of crime services that exist today, which grow in parallel with the demands of cybercriminal syndicates.

Examples of crime services and corresponding rates (USD) include:

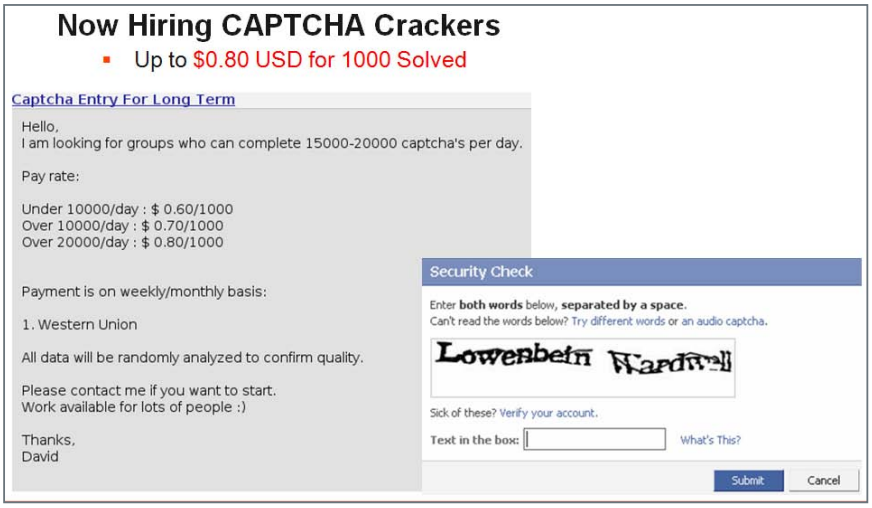
- **Consulting services such as botnet setup** ($350-$400)
- **Infection/spreading services** (~$100 per 1K installs)
- **Botnets & Rentals** [Direct Denial of Service (DDoS) $535 for 5 hours a day for one week], email spam ($40 / 20K emails) and Web spam ($2/30 posts)
- **Quality Assurance vs. Detection** (Crypters, Scanners - $10 per month)
- **Affiliate Programs** ($5k per day is possible)
- **Onshore & Offshore Hosting – Virtual Private Servers** ($6 per month),
- **Bulletproof/Fast Flux hosting and** (VPNs & reverse proxies ($3 per month)
- **Blackhat Search Engine Optimization (SEO)** ($80 for 20K spammed backlinks)
- **Inter-Carrier Money Exchange & Mule services** (25% commission)
- **CAPTCHA Breaking** ($1/1000 CAPTCHAs)—Done through recruited humans
- **Crimeware Upgrade Modules**: Using Zeus Modules as an example, range anywhere from $500 to $10K

Technical support or communication through these services is generally offered through ICQ messaging or the like. The wide range of available services also includes highly specialized "Cloud Cracking," which offers high performance password cracking at a low cost and significantly reduces time it takes to uncover strong passwords. Altogether, 300 million attempts, which takes about 20 minutes, costs about $17. Cloud cracking has been around for a few years, but FortiGuard Labs are seeing a significant increase in speed offered by these services at a reduced cost.

What could take weeks using standard desktop password cracking software such as Jack the Ripper only takes a few minutes now using specialized applications and hardware. And what used to take years, can now be done in hours. This is possible through distributed computing, generally available by harnessing the power of a botnet – thousands, if not tens of thousands of infected machines' computing power.

R & D

As with many growing enterprises, the backend systems behind the scenes of crime services is varied and complex. Powering the attacks are extensive R&D organizations creating custom-ordered code. These organizations produce private botnets, fake antivirus software, ransomware, deployment systems and exploit code, whatever the syndicate needs to attack and infect systems. Before releasing, like any legitimate organization, code is



Example of recruitment of contractors to crack CAPTCHA authentication

Cloud Cracking enables cybercriminals to attempt hundreds of thousands of password in minutes.

put through a QA process to ensure all is functioning and potentially evading security detection.

Hosting Providers

Hosting providers are crucial to the success of cyber criminals, as affiliates need locations on which to store the attack content (such as exploit code, malware and stolen data). These may be official hosting providers or services posing as hosting providers that actually offer up compromised systems for storage. Typically, hosting providers are offshore (often found in political safe havens such as Russia and China) and turn a blind eye to the people purchasing the space and the illicit content being stored on them. However, there have been some instances of US hosting providers in the past linked to malware, such as California-based McColo (which was eventually taken offline).

Closing illegally-operating hosts is a difficult task, because oftentimes, the traced malware is tracked to legitimate servers that have unknowingly been compromised. When discovered, threat researchers typically attempt to notify an ISP in question that they're hosting illegal operations, but, more times than not, those calls for investigation are ignored. Unless it is a very large operation, government resources are often constrained and not available to take down the rest.

Domains

Cybercriminals are constantly creating new domains after old ones are closed to avoid detection and to maintain a steady revenue stream. When a malicious domain is discovered, it is not always easy to take down – sometimes the domain registrar itself will be unresponsive to a takedown request. The cycle of closing old sites and opening new ones more often than not plays out like a never-ending and ever-expanding game of "Whack-a-Mole." In other words, for every malicious domain taken down, two more just like it pop up to take its place. Domain registration is often automated – purchased through the use of stolen credit cards. Naming conventions are also precalculated in some cases through domain generation algorithms (DGAs), where malicious domains are registered on a daily basis. In order to do this, a relationship must exist with the domain registrar so the registering party will not be blacklisted.

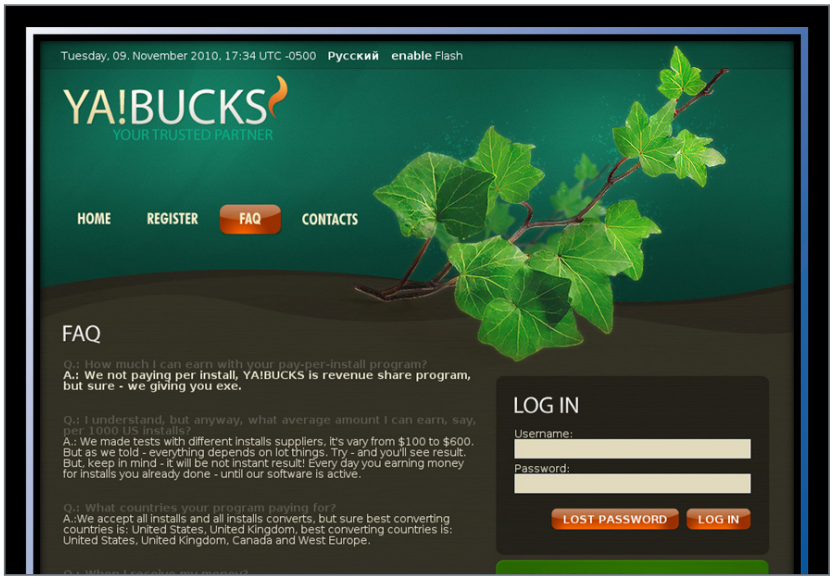
Growing the Business

Meanwhile, in order for a crimeware syndicate to grow their operation over time, they need to connect with other organizations and distributors. Fortinet has found evidence of a Virut botnet syndicate looking to grow their own botnet through the use of other organizations' botnets. Due to competition, merger and acquisitions are already occurring. The most recent example of this is with Zeus & SpyEye.

Money Mules

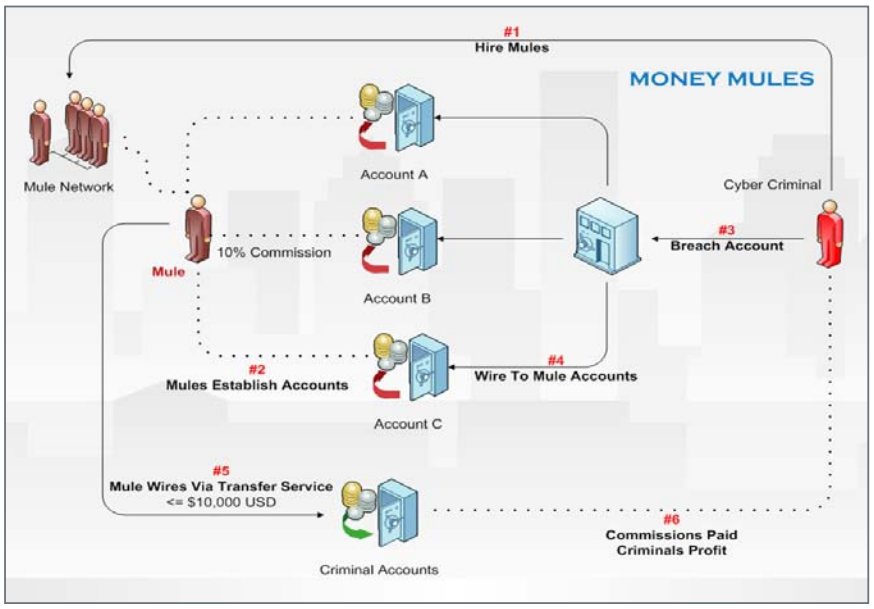
To help grow an illicit organization, leaders employ money mules, people who are knowingly or unknowingly used to launder a crime syndicates' ill-gotten gains. Money mules are often recruited through advertisements and are used to anonymously move money from one country or bank account to another. This money shuffling is typically done through anonymous wire transfer services such as Western Union, Liberty Reserve, U Kash and WebMoney.

Proxied or anonymous wire transfers are important techniques to avoid detection, because transactions are often fragmented into smaller batches to avoid triggering alerts mandated by anti-money laundering laws. By using several mules, anonymous services and various bank accounts, it is harder for authorities to trace funds and places legal responsibility on the mules themselves. *(See Figure 4)* FortiGuard Labs has seen recent evidence of criminals launching targeted recruitments for specific regions (and their local banks). These are through money mule recruitment campaigns, posed as account receivable positions on various career/personal sites. The money mule



An example of a revenue sharing model for infecting systems

layer is similar to other techniques employed for anonymity. A layered communication infrastructure is often built into any cyber criminal operation. For example, infected machines do not directly speak to the operators of a criminal syndicate. Rather, they will go through intermediate machines, which bounce communication off others before reaching the criminal operator. This is usually done through other compromised machines using technology such as a virtual private network (VPN). Much like the money mule process described above, the goal is to complicate tracing efforts. For botnets, a main server typically exists that will receive commands through intermediate (anonymous) servers – this main server is referred to as the "Mothership."



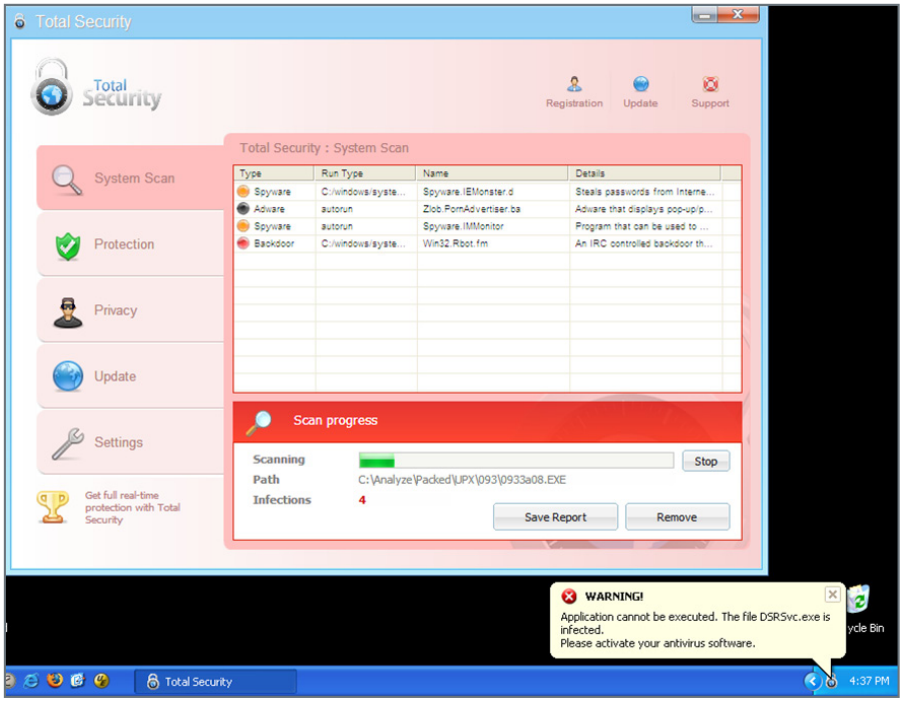
How Zeus botnet operators utilize money mules

Developing a Business Model

Crimeware syndicates, in order to survive, must possess a comprehensive business model and monetization strategy because even an illegal company needs to 'pay the bills' in order to function on a day-to-day basis. One such example is the "pay-per-click" model, where a payout is given to a member of the infantry for traffic generation to an advertisement site. This is generally done through malware installed on a system, which receives commands on the sites to go to and the advertisements to click on. Revenue for those advertisements is given back to the malware author. There's also a "pay-per-install" model, in which payout is given to infantry when machines are infected with software, usually by batches of one thousand.

Another model, known as "pay-per-purchase," is when a payout is given to a member of the infantry when infected users purchase fake software such as fake antivirus and/or fake products, such as counterfeit pharmaceuticals. Fake antivirus rewards affiliates by scaring the victim into thinking their machine is infected and needs to be cleaned by a product offered by criminals. The victim will typically pay between $50 and $100 for the privilege of removing the scareware.

Ransomware, which actually encrypts data on an infected user's machine, is a new trend that seems to be superseding fake antivirus in popularity among cybercriminals. This type of malware uses the pay-per-purchase business model and charges victims a fee to get their data back (typically $100 USD). This is generally more effective, since in cases of strong Ransomware, the user must pay to have their data back – it is the only way to reverse the encryption.



A typical ransomware infection

There have also been instances of corporate blackmail, a similar concept to ransomware. Instead of giving data back to the victim, the victim is threatened that the data will be released to a public domain unless a fee is paid. Depending on the target and type of data, this can range from hundreds to hundreds of thousands of dollars.

Rent, Buy or Lease?

Cybercriminals also reap profits by renting or leasing of hacking tools to third parties, often for a set price but subject to negotiation. As previously mentioned, tools touting more elaborate and evasive features will command the highest price:

- **Botnets**: Features include, broadcast command & control, keylogging, download and spam. Examples include Zeus/ZBot ($700 for old version, $3,000 for the new) and Butterfly ($900)
- **Simplified botnets**: Features include download and execute malicious code. Used primarily for rentals/crime-as-a-service. Example includes Bredolab (starts at $50)
- **Remote Access Trojans (RATs)**: Features include targeted attacks, with screen shot and webcam feed capabilities. Examples include Gh0st Rat, Poison Ivy and Turkojan ($250)
- **Exploit Kits**: Feature enables exploiters to attack users via Websites. Examples include GPack, MPack, IcePack and Eleonor ($1K-$2K)
- **Crypters, Packers and Binders**: Features enable an attacker to obfuscate binary code, piggyback code and generally avoid detection ($10-$100)
- **Source code**: This is generally free and available to anyone through well known kits posted on underground forums. It can be leaked from private/controlled versions of code in a case where hackers attack hackers. Source code is the root of all malicious code that exists today and a big reason why new threats keep coming up – it can be copied, modified and molded into a new threat with relative ease. One example is Zeus, which has had manifold modifications since its release (and new variants continue to appear) due to the ease of access to the source code and the amount of documentation that exists describing how to modify it.

Money Management

As with legitimate businesses, syndicates need to keep track of key metrics, such as how many infected machines they're commanding, how many accounts they have cracked, how much money in those cracked accounts they've transferred and so forth. They utilize commercial business process management tools, financial systems, databases and Web portals to manage everything from software development to accounts payable.

How to Stop it

The challenge to stopping the growth of Crimeware today is the inability to prevent its manufacturing. Trying to stop the product development process constitutes a never-ending game of cat and mouse. Once made available to the public, malicious software code is incredibly difficult to pull down.

Governments have been relatively powerless to stop it, since the number of threats outnumber the number of government resources to investigate and take down those threats. Resources become even more constrained when it comes to actually prosecuting cybercriminals. Today, FortiGuard Labs researchers are seeing more individuals and organizations helping to create/refine/evolve malware. There are simply more players in the game because of the consumerization of Crimeware and Crime Services – anyone can make a quick buck without having to be technically adept. It's getting worse--Fortinet processes millions of samples of malware monthly, and the volume is currently 3X greater than it was in December 2008. This increase puts a greater demand on security vendors/researchers to stay abreast of the latest crimeware threats.

Despite this grim outlook, there have been some successes in fighting back against some of the larger threats. For example, both the Conficker and Mariposa botnets were so large that task forces were assigned to deal with them (Conficker & Mariposa working groups).

One success story was the Butterfly/Mariposa botnet takedown in March 2010. Altogether, the botnet had infected more than 12 million PCs, more than half of which belonged to Fortune 1,000 companies and 40+ major banks. One developer and five associates were arrested.

A prominent Zeus/Zbot network was also officially taken down in September of 2010. During the action, 11 Eastern Europeans were charged, 73 money mules around the world were charged, 37 of which were alleged to have

transferred over $3 million, 36 alleged to have transferred $860,000 from 34 corporate and individual victims, and it was discovered the mules came to the US on legitimate work Visas. The Dutch High Tech Crime Unit disrupted Bredolab in October 2010—an undertaking that saw one Armenian man arrested. He had control of 143 servers that were in control of 29 million infected PCs. Dutch prosecutors allege that he was making $139K per month just on spam rentals. As of November 2010, other Bredolab botnets still existed.

Koobface was taken offline several times, once in November 2010 when UK ISP Coreix unplugged access to Koobface command servers. This was a limited success story, since the botnet came back online four days after it was taken offline. This is because of the technology Koobface employs, which allowed the operators to quickly rebound. In this situation, only middle layer servers were taken offline, while a "Mothership" remained online, allowing operators to regain control. There were also no arrests made since this was purely an infrastructure takedown at the time. The operators were still at large since a full investigation had not commenced. It is important to fully understand all the components of a botnet before a proper takedown can occur.

With the help of Microsoft Digital Crime Unit, the Kelihos botnet, which was rumored to have as many as 40,000 bots, was taken offline in September 2011. This was a collaborative effort between Microsoft and the US government to bring Kelihos operators to prosecution. Unfortunately, prosecution takes some time and after the initial takedown, it only took a few days before a new version was discovered functioning and growing its infected base again.

Stop the Domain Registrations

Aside from dismantling a botnet's command and control center, another preventive way to curb crimeware is to not allow people to register these domains. As much as China has been chided for its lax cyber policing, the country has taken several positive steps towards legitimizing domain registration for their domains (.CN), including relying on paper-based registration forms to better screen and maintain quality over who is registering domains. Also, the Conficker Working Group also helped to filter out domains in advance before they could be registered to prevent the spread of that particular botnet.

However, maximum effectiveness for domain management requires global participation. An international body that would act as a mediator for domain registration disputes and to dispatch resources to appropriate regions and share information of new trends would be best suited for this role. At the highest level, there needs to be a central reporting channel where the private sector, which would include vetted security vendors, can send their research on malicious domains – and be heard.

Currently there is no centralized reporting structure in place (although there are some initiatives in progress) for cyber threat related incidents. There are many individual computer emergency response teams (CERT), and they respond to incidents as quickly as they can. The problem is that dispatchers only respond to incidents in their jurisdiction. When an incident is reported to a region where the appropriate law-enforcement agencies do respond, it's often discovered that those officers are poorly trained and/or don't have the resources to follow through on cybercrime in general and crimeware in particular. Organizations like FIRST aim to bring these CERTs together to act in unison on any given threat, but more people need to be aware of where to go and what to report when a threat is discovered.

How to Fight Back

Realistically, the most effective way to secure a business today from crimeware is from the inside out. There is no central government agency in any country that can prevent the spread of crimeware. Organizations need to take protective steps to prevent the spread of crimeware among its users and customers. That means developing a comprehensive and layered security strategy that consists of a variety of elements, including intrusion prevention, botnet and application control, Web filtering, antispam, and antivirus. It is also incumbent upon an organization to educate its users about security best practices, while creating adequate enforceable mechanisms for security policy violations. FortiGuard Labs has a regular security blog (http://blog.fortiguard.com) and threat portal to highlight

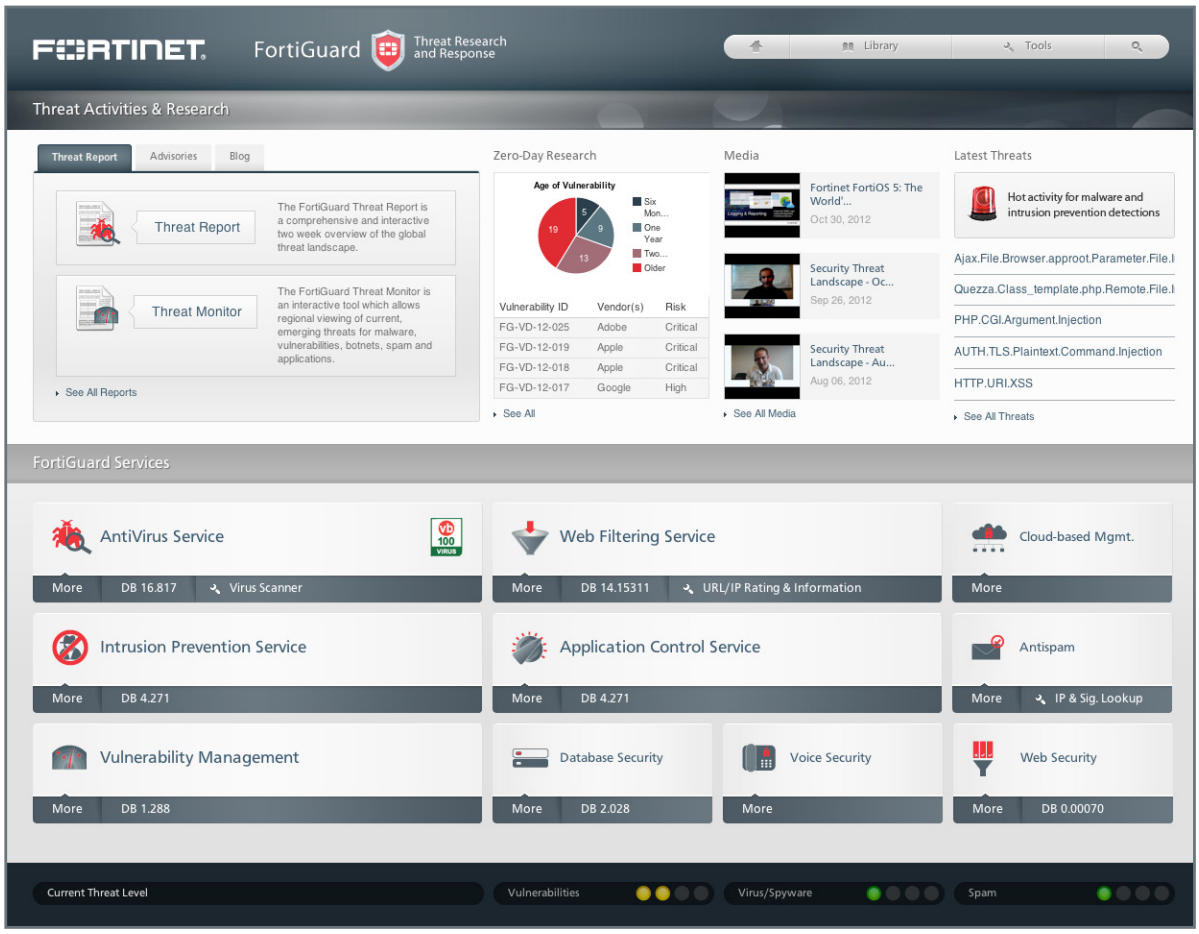


FIgure 5: FortiGuard Threat Research and Response website

the latest breaking threats (http://www.fortiguard.com *See Figure 5*). For administrators, groups such as ISACA are worth evaluating in order to stay on top of best security practices in relation to the modern threat landscape.

Cybercrime is well-established, well-equipped, and well-funded. It employs armies of employees, contractors, and partners. It constantly generates new malicious programs designed to circumvent security mechanisms, trick users into installing malware and divulging credentials and stealthily steal valuable information.

However, it's not insurmountable. As history has shown, collaborative efforts have toppled some of the world's most powerful botnets and crime rings and will continue to do so. While new cybercrime syndicates will continue to emerge and proliferate, organizations that arm themselves with a solid, multi-layered security strategy and security best practices are doing their part in the effort to reduce the effectiveness of cybercrime. ■

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480